Third Party Information Technology Security Questionnaire

Security Policy and Organization

1. Please provide a copy of your organization's cyber security policy.
2. Are security requirements explicitly detailed in the service contract, including an Incident Response/Threat Management process and Security Vulnerability Management process?
3. How do you ensure that the security policy, standards and procedures are current?
4. How often are risk assessments performed?
5. Please provide a clear definition of roles and responsibilities for security within the organization structure.

Personnel Security

1. Do you employ comprehensive employment contracts including a confidentiality clause, reference to security responsibilities, penalties/disciplinary proceedings for non-compliance, etc.?
2. Do you regularly review staff compliance for security responsibilities and other legal and regulatory requirements?
3. Do you have adequate backup of all key roles and responsibilities?
4. Is a regular review of system access rights conducted?
5. Are automated expiration dates for contractor sites and system access used?
6. Do you perform detailed background checks on employees with access to sensitive/customer information?

Physical Security

1. Is access controlled at all times?
2. Is all access recorded and authorized by designated management?
3. Is all visitor access authorized, justified and supervised?
4. Do you use 24x7 on-site security guards?
5. Is CCTV monitoring of external perimeter and external access points used?
6. Is access to the computer room(s) restricted?

7. How do you protect the computer room(s) against:

    a. Water
    b. Fire
    c. Power surge
    d. Power loss

Media and Data Security Disposal

1. Please provide your policy on the classification and safe handling of third party (e.g. NREL) data.

2. Describe your methods of permanent physical data erasure and destruction.

3. Please describe your system backup and data retention policy with regards to third party data.

4. Will computing and storage resources be shared or dedicated to NREL?

5. Describe your policy and procedure for customer notification in the event of significant security events.

6. How long are system logs and audit trails maintained?

Platform Security

1. Describe your user account and password policies for:
    a. Local users
    b. Privileged users
    c. External users (NREL)

2. Describe your policy for creating a secure system with regards to:
    a. Default accounts
    b. Default passwords
    c. Unused applications/ports

3. Do you use Anti-virus, spyware, IPS/IDS, and spam protection?

4. Do you have configuration management techniques and policies in place?

Application Security

1. Do you use a separate audit log server for the applications?

2. Describe your policy for application accounts with regards to:
    a. Multi-factor authentication
    b. Encryption for authentication
    c. Lockout following # of failed attempts
    d. Unlocking of locked out accounts
    e. Disabling of inactive accounts

3. Are backups of application data encrypted?

4. How are application vulnerabilities identified, tracked, and mitigated?

Network Security

1. Briefly describe your existing Firewall infrastructure with regards to:
    a. Use of DMZs
    b. Redundant clustered Firewalls
    c. Stateful inspection technology
    d. Access control
    e. Change management
    f. Default-Deny policy

2. Do you use routers that enforce ACLs?

3. Will specific firewall rules be implemented for NREL's activity?

4. Do you use host based and network based IDS / IPS systems?

5. Who will be responsible for incident escalation and notifying NREL in the event of a security breech?